REMARKS

Claims 1-7, 9-19, 21-31 and 33-47 are all the claims pending in the application. By this Amendment, Applicant amends claims 1, 13, 25, 37, and 43 to further clarify the invention. In addition, Applicant adds claims 44-46.

Statement of Substance of the Interview

Applicant thanks the Examiner for the courteous telephonic interviews. The Statement of Substance of the Interview is as follows:

During the Interview, independent claim 43 was discussed in view of the prior art of record. In an attempt to expedite the prosecution in the present application, the Examiner and the Applicant discussed possible amendments to the independent claims that would more clearly distinguish the present invention set forth in the independent claims from the prior art of record.

In particular, the Examiner appeared to agree that the combination of verification, *i.e.* "when the received user name and the computer identifier matches the parsed user name and the computer identifier, using the parsed server user identifier to acess the server," and the use of the generated authentication key to access the data store, *i.e.*, "the user accesses the data store via the server using the generated authentication key, and wherein, when the server user identifier changes, a new authentication key is generated for the user and the user accesses the data store via the server using the new authentication key" is not taught or suggested by the prior art of record.

In view thereof, Applicant amends the claims 1, 13, 25, and 43 to further clarify the invention. In addition, in order to provide more varied protection, new claims 44-47 are added.

Claim Rejections under 35 U.S.C. § 103

Claims 1-7, 9-19, 21-31, and 33 to 43 stand rejected under 35 U.S.C. § 103(a). Applicant respectfully traverses in view of the following remarks.

Stallings and Bryant

In particular, claims 1-7, 9-11, 13-19, 21-23, 25, 31, 33-35, 42 and 43 are now rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter "Stallings") in view of Bryant "Designing an Authentication System: a Dialogue in Four Scenes" (hereinafter "Bryant"). Of these rejected claims, only 1, 13, 25, and 43 are independent. This response will initially focus on these independent claims

Among a number of unique features of claim 1, not taught or suggested by the prior art, is "...when the received user name and the computer identifier matches the parsed user name and the computer identifier, using the parsed server user identifier to access the server, wherein the user accesses the data store via the server using the generated authentication key, and wherein, when the server user identifier changes, a new authentication key is generated for the user and the user accesses the data store via the server using the new authentication key."

In the conventional unified logon systems, each client computer connected to a database server computer needs to have a corresponding user identifier and password created on the server computer, in addition to having a user name and a password to log onto the client computer. This requirement creates an administrative nightmare because of maintaining and managing all the client user names and passwords with the corresponding server user IDs and passwords Moreover, when a server password or ID is changed, the system administrator needs to notify the

users of their new password or server ID, creating additional security risk of the message being intercepted by hackers.

In the method as set forth in claim 1, however, the authentication key is generated "based on a user name and a computer identifier" and the authentication key "includes a server user identifier." As a result, the administrator need not forward the server ID to the user. Instead, the server ID is sent to the user in an authentication key based only on the user name and a computer identifier received from the user. The user will use this authentication key to access the server, *i.e.*, "when the received user name and the computer identifier matches the parsed user name and the computer identifier, using the parsed server user identifier to access the server."

Moreover, one server ID can be used for a number of users, and each user will still have a unique authentication key. Finally, "when the server user identifier changes, a new authentication key is generated for the user and the user accesses the data store via the server using the new authentication key." Accordingly, the notification process is more secure and easier to implement for the administrator. This passage is provided by way of an explanatory example only.

Stallings, similar to the conventional techniques described above, teaches a client sending a server ID, along with the client name and password. These server ID, client ID and client password are encrypted by the authentication system to create a ticket for the client. The client then uses this ticket to gain access to the server. The server verifies client ID with the encrypted client ID in the ticket. If the two match, access to server is provided (page 326 of Stallings). This is no different from the conventional techniques described in the background of the

invention. When the administrator changes the server ID, a new server ID has to be sent to the user, creating additional security risk of the message being intercepted by hackers.

Bryant, is no different from Stallings, except that Bryant's ticket includes a network address of the client computer, which is checked against the network address of the client, which sent the ticket (page 5 of Bryant). Thus, this design guards against the interception of the ticket and attempts to send it from a different computer. Bryant, however, fails to address the problem of changing server IDs for the user.

The Examiner acknowledges that both Stallings and Bryant fail to teach or suggest the authentication key including a server user identifier. The Examiner, however, now alleges that such an inclusion would be an obvious enhancement. For support, the Examiner cites systems such as Windows, NT, Unix, Linux (see pages 5-6 of the Office Action). Applicant respectfully disagrees. If the Examiner decides to maintain this rejection, Applicant respectfully requests the Examiner to substantiate this argumentation with additional references for the following reasons.

Stalling and Bryant do not teach or suggest having a server user identifier in the ticket. The systems mentioned by the Examiner, similar to the conventional techniques described in Applicant's specification, provide the user, *e.g.*, via email, with a user identifier and a password, which the user has to enter to access the service. The systems mentioned by the Examiner do not teach or suggest any kind of encryption for this identifier and this password.

Moreover, none of these systems including Stalling's and Bryant's system recognize the problem of managing user name and password with the server identifier and password and as such do not provide any suggestion to place the server user identifier into a ticket. Finally, his allegedly obvious enhancement would require significant modifications to the system of

Stallings and Bryant. That is, instead of simply identifying the user, the systems would have to recognize that an additional key should be extracted and used to access the server. In short, Applicant respectfully submits that including a server user identifier along with the user name is clearly not an obvious enhancement and but for the present invention there is no suggestion to include the server user identifier into the ticket as taught by the combined teachings of Stallings and Bryant.

Moreover, even assuming *arguendo* that including a server ID is an obvious enhancement, the combined teachings Stallings and Bryant still fail to teach or suggest that "when the received user name and the computer identifier matches the parsed user name and the computer identifier, using the parsed server user identifier to access the server." That is, in Stalling and Bryant, once the user is verified, he is permitted to access the server. There is no teaching or suggestion to use a parsed server user identifier to access the server. Moreover, there is no teaching or suggestion that when the server ID changes, instead of sending to the client a new server ID (creating additional security risk of the message being intercepted by hackers), creating a new authentication key and providing the user with a new authentication key as opposed to a new server ID.

Therefore, "...when the received user name and the computer identifier matches the parsed user name and the computer identifier, using the parsed server user identifier to access the server, wherein the user accesses the data store via the server using the generated authentication key, and wherein, when the server user identifier changes, a new authentication key is generated for the user and the user accesses the data store via the server using the new authentication key," as set forth in claim 1 is not suggested or taught by the combined teachings of Stallings and

Bryant, which lack any suggestion of including the server user identifier into the authentication key, using the parsed server user identifier to access the data store, and generating a new authentication key for the user when the server user identifier changes.

For at least these exemplary reasons, Applicant respectfully submits that claim 1 is patentable over the combined teachings of Stalling and Bryant. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject mater of claim 1. Since claims 2-7, 9-11, and 42 are dependent upon claim 1, they are patentable at least by virtue of their dependency.

Next, Applicant respectfully traverses this rejection with respect to independent claims 13, 25, and 43. These independent claims recite similar features to the features argued above with respect to claim 1. Therefore, arguments submitted with respect to claim 1 apply with equal force here. For at least substantially the same reasons, therefore, Applicant respectfully requests the Examiner to withdraw this rejection of independent claims 13, 25, and 43. Claims 14-19 and 21-23, and claims 26-31 and 33-35, are patentable at least by virtue of their dependency on claims 13 and 25, respectively.

Stallings, Bryant, Fuh, VeriSign, and Schneier

Claims 12, 24 and 36 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant and further in view of U.S. Patent No. 6,463,474 to Fuh et al (hereinafter "Fuh"). Claims 37-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant further in view of VeriSign "Certification Practice Statement" (hereinafter "VeriSign"). Alternatively or in addition, it seems that claims 38-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stalling, Bryant, Fuh, and VeriSign (see

page 11 of the Office Action); clarification with respect to claims 38-40 is respectfully requested. Finally, claim 41 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant and further in view of Schneier Applied Cryptography (hereinafter "Schneier"). Applicant respectfully submits that Fuh, VeriSign, and Schneier do not cure the deficient teachings of Stallings and Bryant. Therefore, claims 12, 24, 36, 37-41 are patentable at least by virtue of their dependency.

In addition, claim 37, now recites: "wherein the generated authentication key for access to the server is sent to a user, and further comprises a server password, and wherein when the server password changes, a unique new authentication key based on the server user identifier and the server password is sent to the user." Applicant respectfully submits that the combined teachings of Stallings, Bryant, and VeriSign do not teach or suggest these unique features of claim 37. For at least this additional reason, claim 37 is patentable.

Moreover, with respect to claim 41, Applicant respectfully submits that one of ordinary skill in the art would not have been motivated to combine Schneier with Stallings and Bryant. Schneier is very different from Stallings and Bryant. Stallings and Bryant address the problem of access control by a variety of users. In other words, Stallings and Bryant are related to providing a user with a key to access a protected, secure system.

Schneier, on the other hand, is related to splitting a secret (a message) amongst a number of users to prevent each individual user to gain access without the other (page 70). That is, Schneier teaches not allowing an individual user to access a protected item alone. In Schneier, each user must combine his or her part of a message, for example, to access the protected item. The Examiner alleges that Schneier teaches "the user to use the secret to obtain the services of a

server." Schneier, however, teaches just the opposite. Schneier teaches that a user will not be able to access a service and that only a number of users combined (by combining their part of the secret) can access the service, *e.g.*, Trent splits a secret between Alice and Bob, or Alice, Bob, Carol, and Dave (pages 70 to 73).

One of ordinary skill in the art would not have combined Schneier with Stallings and Bryant at least because that would mean that the users would have to get together to access a secret item, alleged service, as opposed to each user obtaining access to the service. In short, one of ordinary skill in the art would not have been motivated to combine the three references in the manner suggested by the Examiner. In addition, one of ordinary skill would not have turned to the secret sharing scheme when designing a Kerberos system so as to provide each user with his or her own individual access. The only reason to turn to Schneier is to try to meet the novel features of claim 41. But for the present invention, there is no reason to turn to the secret sharing scheme of Schneier. For at least this additional reason, claim 41 is patentable over Stallings, Bryant, and Schneier.

New Claims

In order to provide more varied protection, Applicant adds claims 44-46. Claims 44-46 are patentable at least by virtue of their dependency on claim 1.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

AMENDMENT UNDER 37 C.F.R. § 1.111
U.S. Appln. No. 09/513,065
Attorney Docket No.: A8117

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

The undersigned hereby certifies that the above identified correspondence is being facsimile transmitted to Examiner Jung W. Kim at the Patent and Trademark Office on April 26, 2005 at facsimile no. 703-872-9306.

Respectfully submitted,

Nataliya Dvorson
Registration No. 56,616

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: April 26, 2005

Attorney Docket No.: A8117